RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: NCS-T10

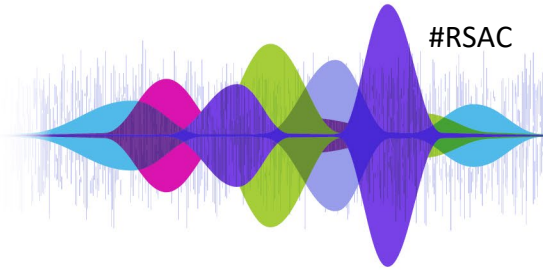
How Can Internet Routing Security Be Improved?

Cecilia Testart

Assistant Professor
School of Computer Science and School of Cybersecurity and Privacy, Georgia Tech
https://www.cc.gatech.edu/people/cecilia-testart

Jonathan Cedarbaum

Professor of Practice for National Security, Cybersecurity, and Foreign Relations Law
George Washington University Law School
https://www.law.gwu.edu/jonathan-cedarbaum



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Internet Routing Insecurity

ZDNet IOT CLOUD AI SECURITY MORE NEWSLETTERS ALL WRITERS

Russian telco hijacks internet traffic for Google, AWS, Cloudflare, and others

Rostelecom involved in BGP hijacking incident this week impacting more than 200 CDNs and cloud providers.

BORDER GATEWAY PROTOCOL —

How 3ve's BGP hijackers eluded the Internet—and made $29M

3ve used addresses of unsuspecting owners—like the US Air Force.

DAN GOODIN - 12/21/2018, 12:

DCD News Analysis Conferences On-Demand Opinions

HOME > NEWS > OUTAGES

Verizon BGP route leak causes Cloudflare customer outages, AWS issues

INTERNET INTELLIGENCE | ORACLE Cloud Infrastructure

June 6, 2019

Large European Routing Leak Sends Traffic Through China Telecom

BORDER GATEWAY PROTOCOL ATTACK —

Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency

Orange Spain Faces BGP Traffic Hijack After RIPE Account Hacked by Malware

Jan 05, 2024 Ravie Lakshmanan

Criminals, Nation-States Keep Hijacking BGP and DNS

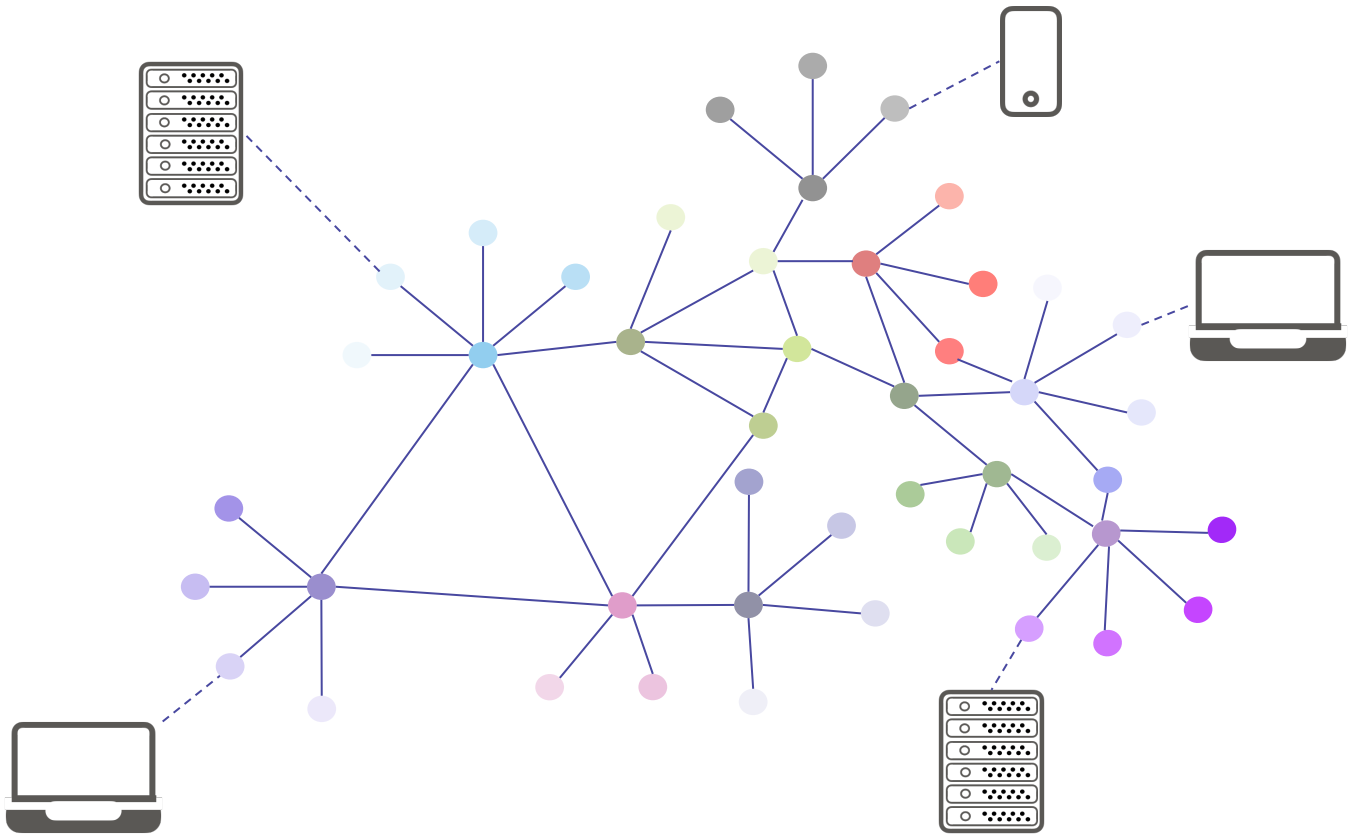
Cloudflare 1.1.1.1 incident on June 27, 2024

2024-07-04

Introduction

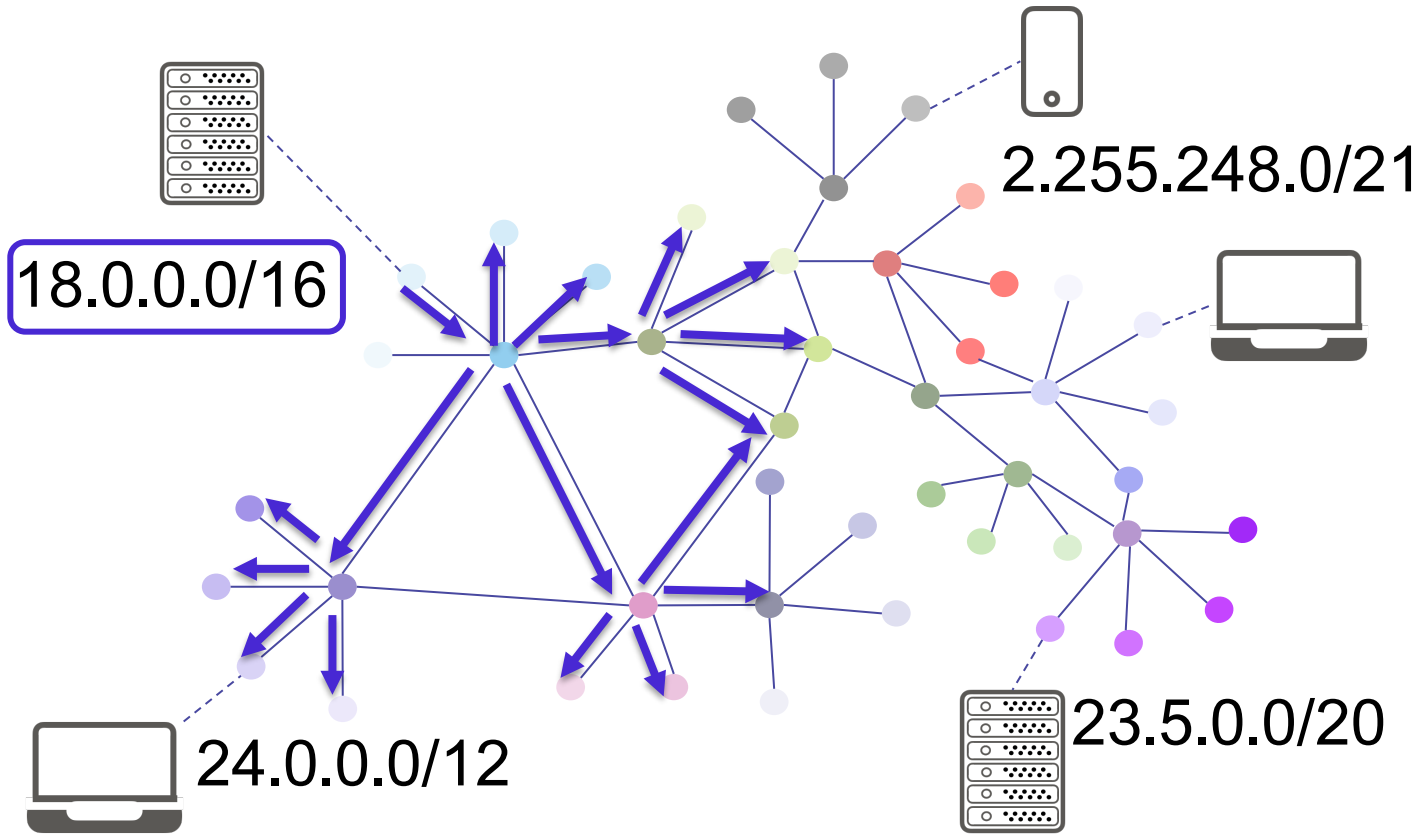
On June 27, 2024, a small number of users globally may have noticed that 1.1.1.1 was unreachable or degraded. The root cause was a mix of BGP (Border Gateway Protocol) hijacking and a route leak.

How Internet Routing Works



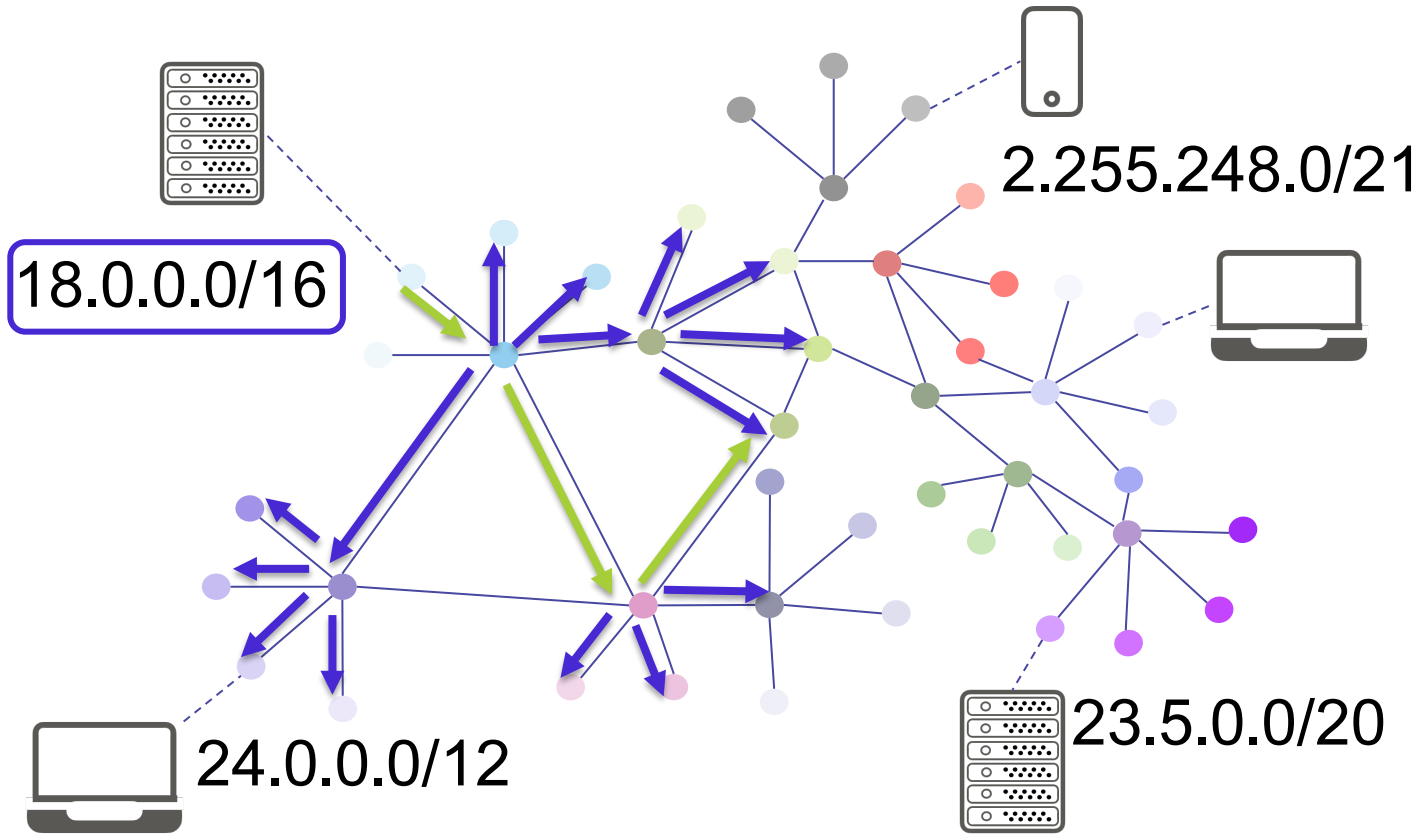
- Networks need to know how to route packets to other networks on the Internet.
- The Border Gateway Protocol (BGP) is the current inter-domain routing protocol of the Internet.

The Border Gateway Protocol (BGP)



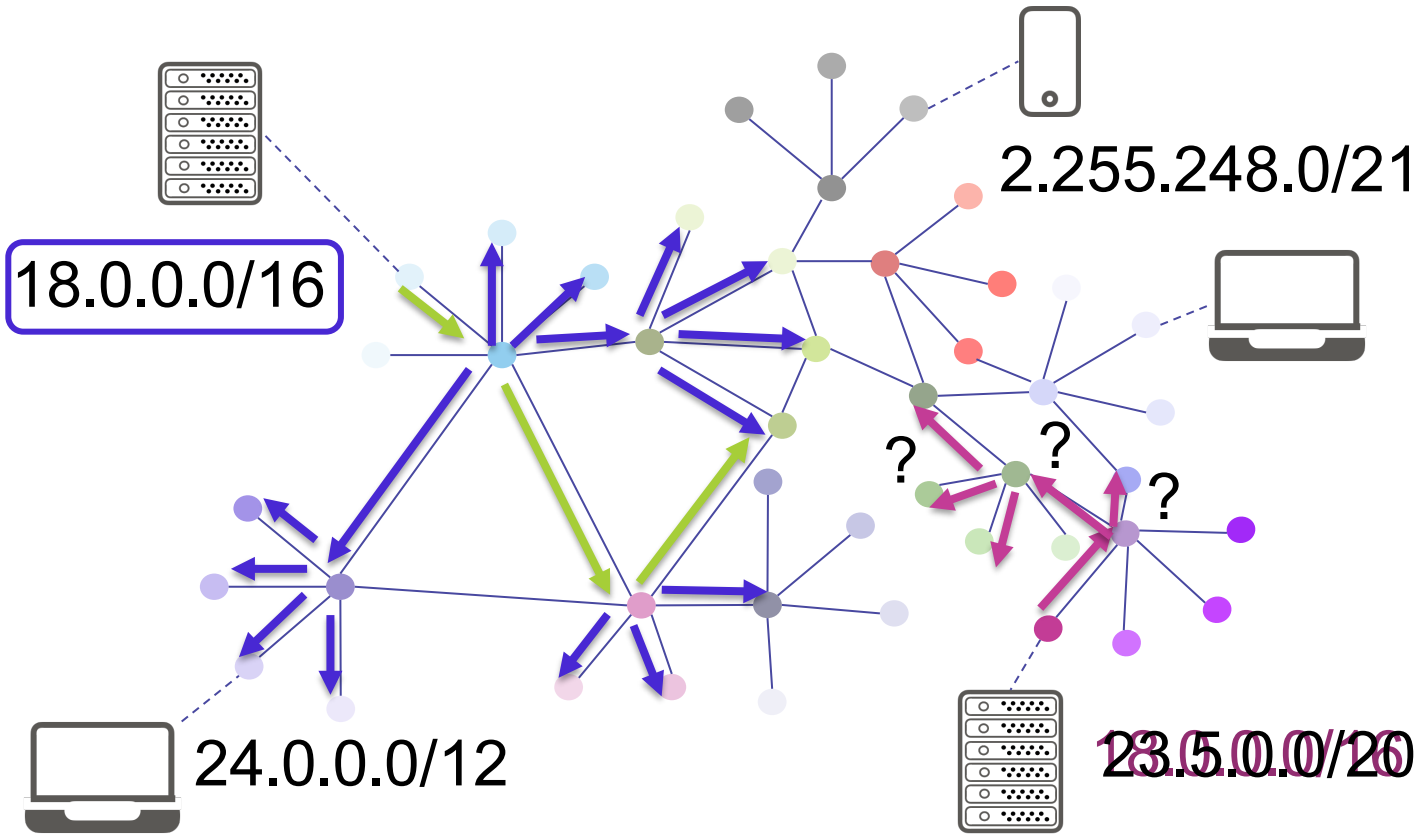
- In BGP, Autonomous Systems (ASes) advertise the IP address blocks they use and the ones they can reach.
- Critical information sent in BGP:
  - IP address blocks (prefixes)
  - Network path (AS path)

The Border Gateway Protocol (BGP)



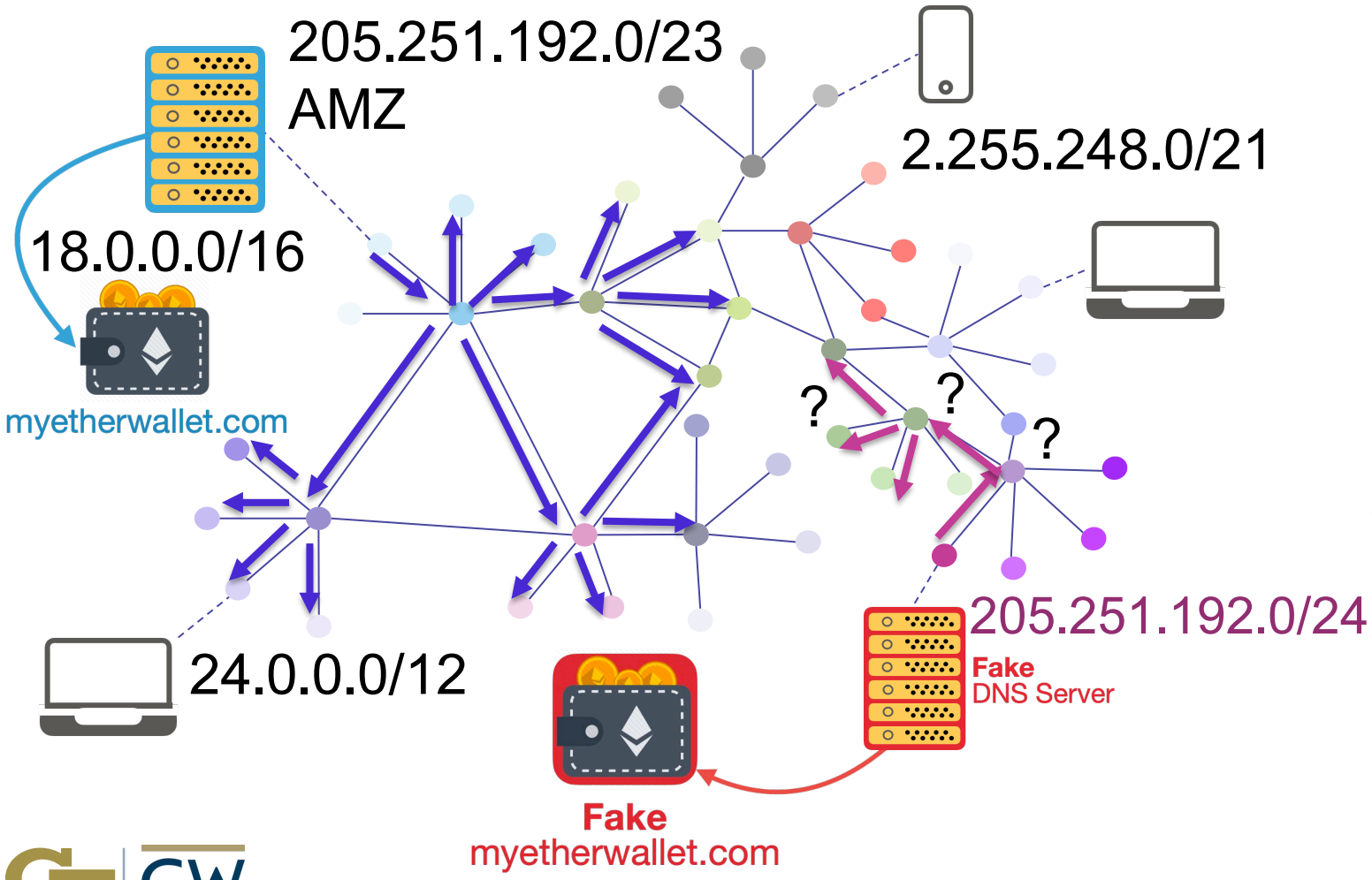
- In BGP, Autonomous Systems (ASes) advertise the IP address blocks they use and the ones they can reach.
- Critical information sent in BGP:
  - IP address blocks (prefixes)
  - Network path (AS path)

The Problem with BGP



- BGP does not have an authentication nor validation mechanism.

BGP Hijack to Steal Cryptocurrencies



- In 2018 and 2022 Amazon was victim of attacks used to steal crypto-currencies from services hosted in its cloud platform.
- BGP hijacks caused Internet traffic to go to the attacker's network.

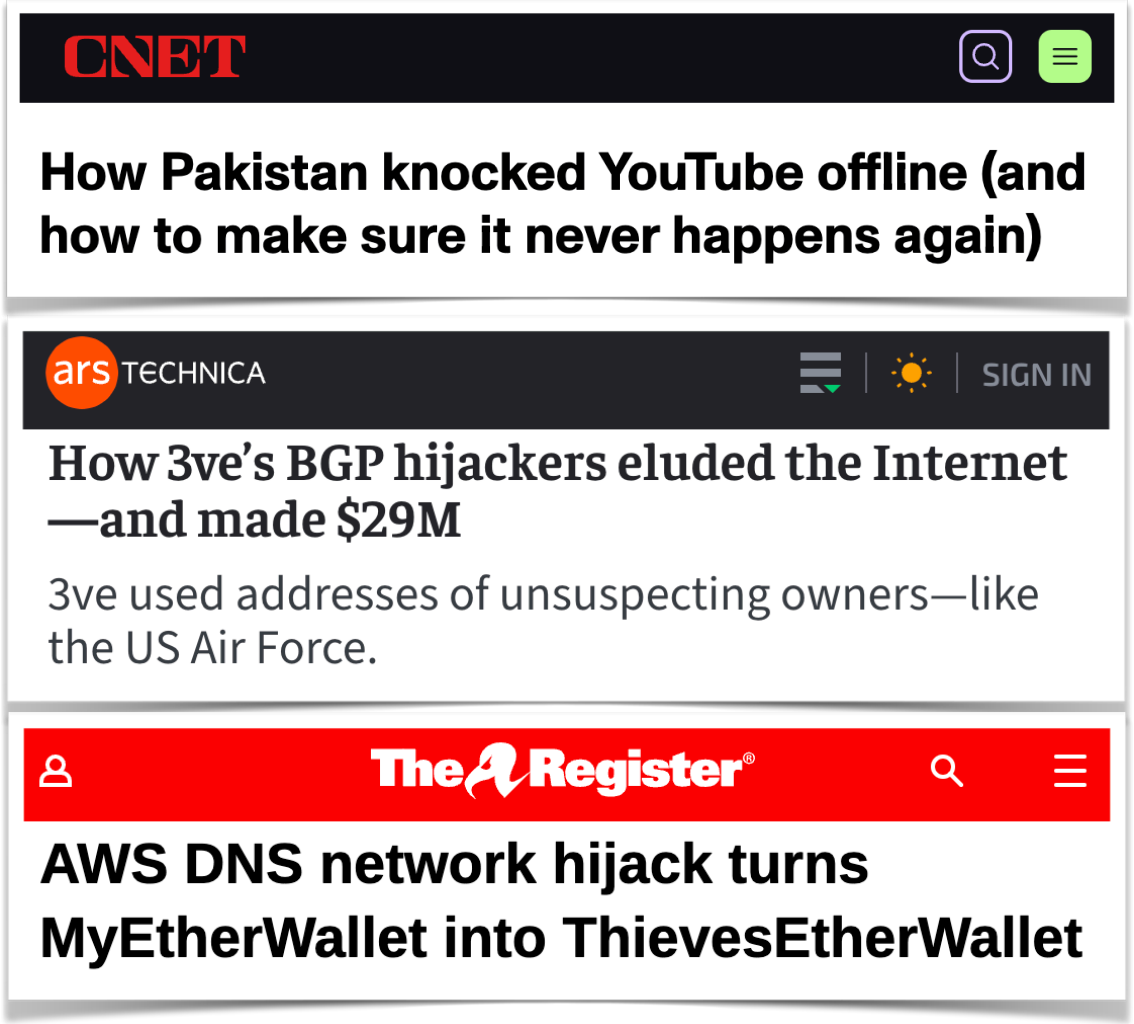
Harms from BGP hijacks

- Attackers can use BGP hijacks to:
  - Make hijacked addresses unavailable (DoS)
  - Send fraudulent traffic from hijacked addresses
  - Impersonate services

Harms from BGP hijacks

Attackers can use BGP hijacks to:

- Make hijacked addresses unavailable (DoS)
- Send fraudulent traffic from hijacked addresses
- Impersonate services


CNET
How Pakistan knocked YouTube offline (and how to make sure it never happens again)
ars TECHNICA
SIGN IN
How 3ve's BGP hijackers eluded the Internet —and made $29M
3ve used addresses of unsuspecting owners—like the US Air Force.
The Register
AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet

From problem to solution

The Problem:

Network/ASes need to identify trustworthy data in BGP.

High-level solution consensus:

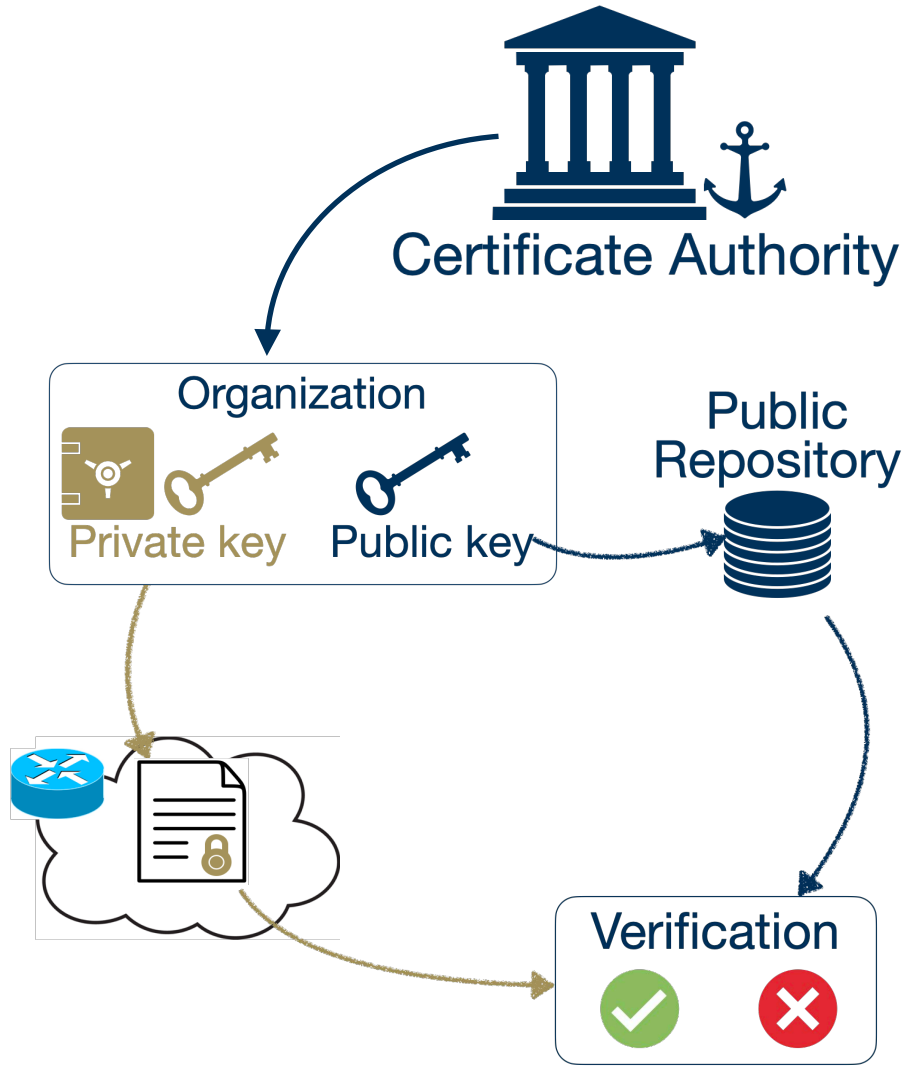
Validate data in BGP against trustworthy data.

Emerging implementation consensus:

Use a specialized Public Key Infrastructure.

Public Key Cryptography for Routing

- Trust Anchor Certificate Authority sets the root of trust.
- Public/Private key pair created.
- Public key goes to public repository, private key is safely kept.
- Private key used to sign records.
- Public key used to verify signature.

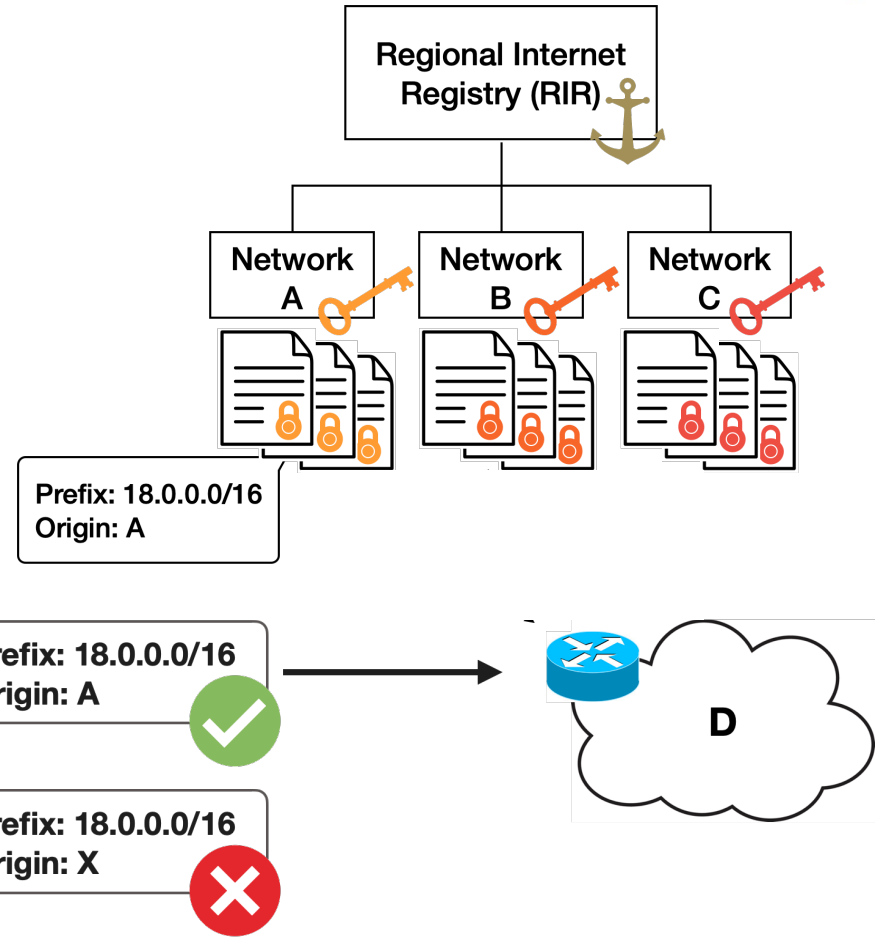


The Resource Public Key Infrastructure

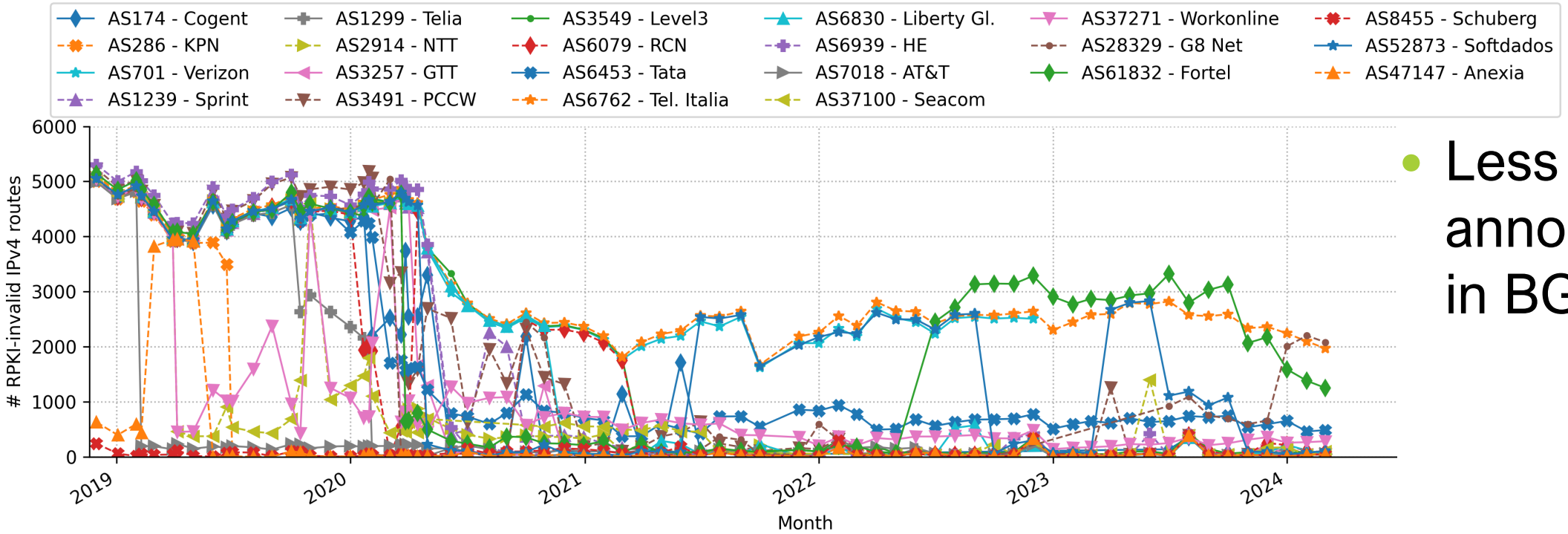
- Framework to secure routing using cryptographic records to validate ***prefix*** and ***origin*** in BGP announcements.

1. Route Origin Authorizations (ROAs) map IP prefixes with valid origins.

2. Networks can use these assertions to validate announcements in BGP (Route Origin Validation, ROV)



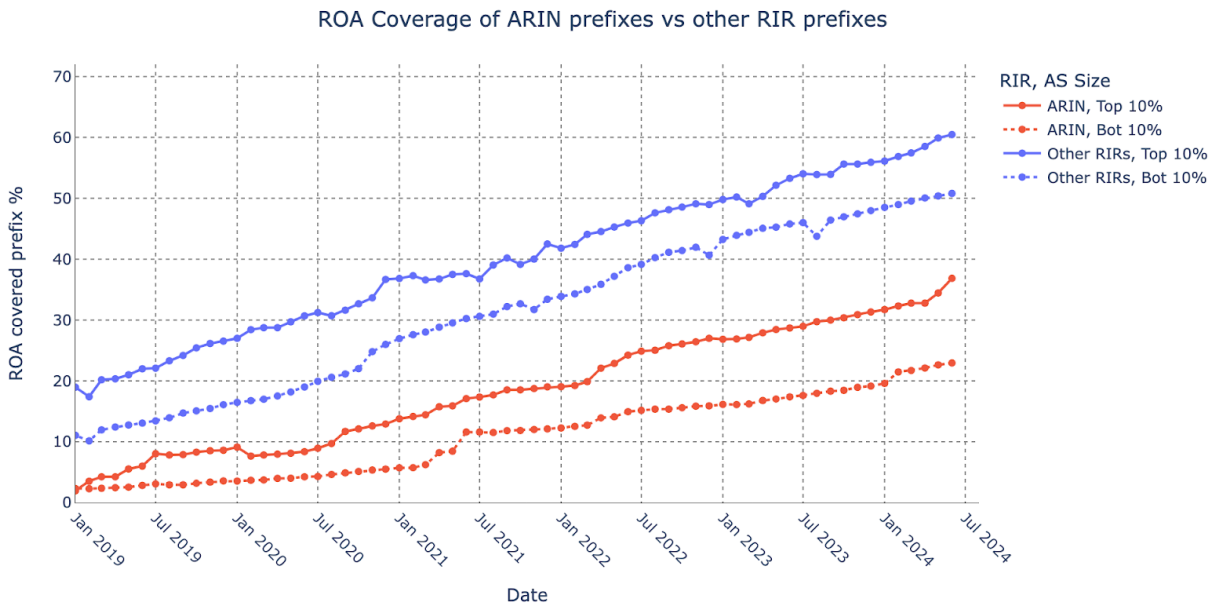
RPKI reduced invalid information in BGP



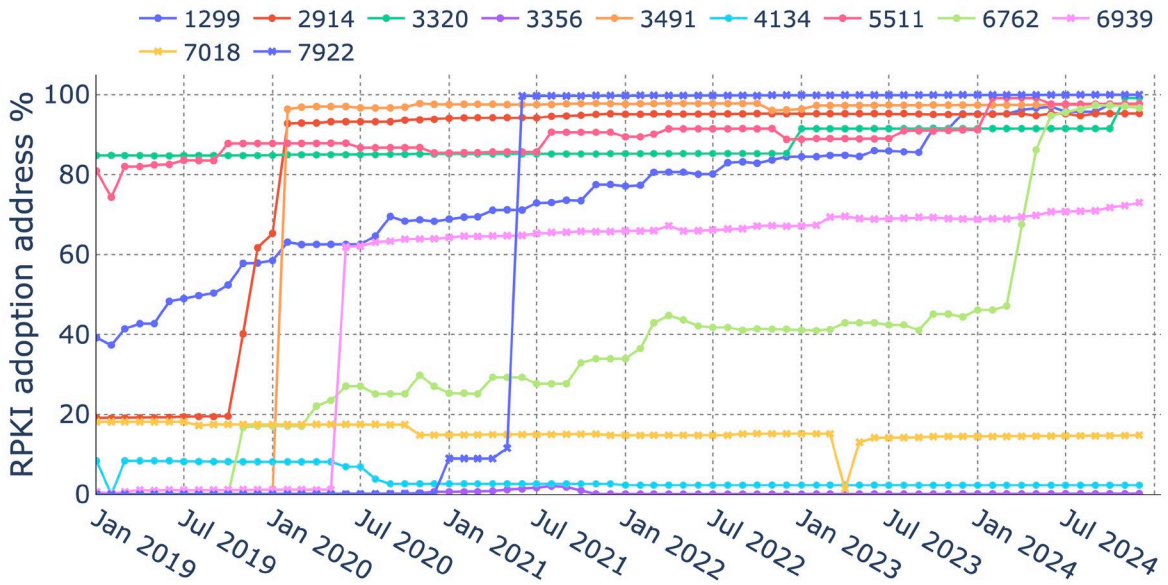
- Less invalid announcements in BGP.

RPKI adoption is challenging

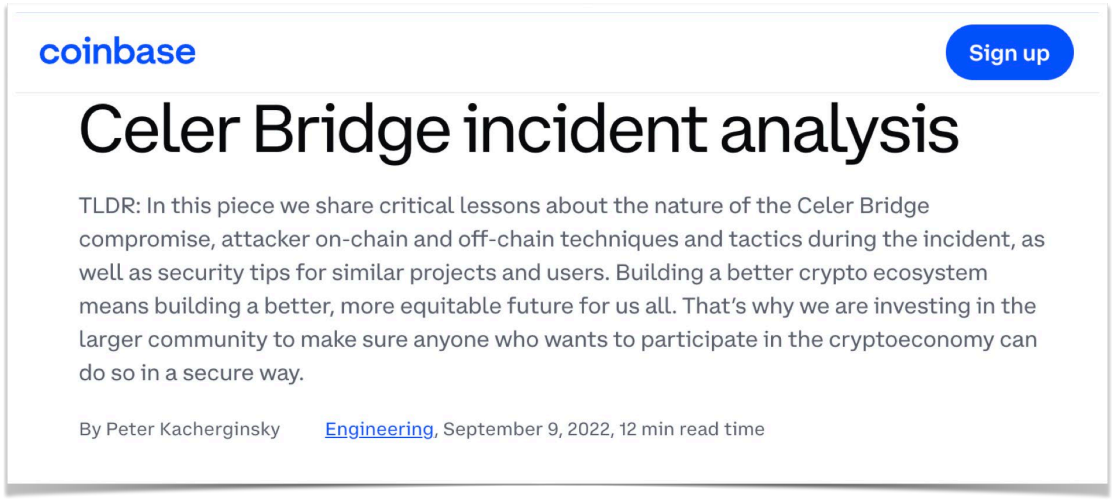
Small vs Large network's adoption



RPKI adoption in select Tier-1s



RPKI has operational issues



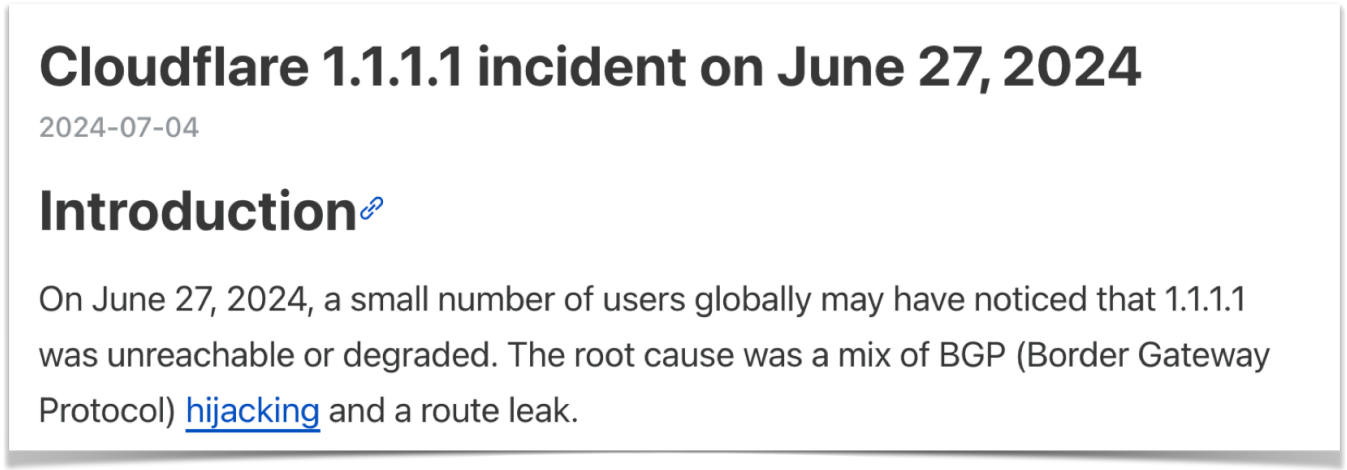
coinbase

Sign up

Celer Bridge incident analysis

TLDR: In this piece we share critical lessons about the nature of the Celer Bridge compromise, attacker on-chain and off-chain techniques and tactics during the incident, as well as security tips for similar projects and users. Building a better crypto ecosystem means building a better, more equitable future for us all. That's why we are investing in the larger community to make sure anyone who wants to participate in the cryptoeconomy can do so in a secure way.

By Peter Kacherginsky Engineering, September 9, 2022, 12 min read time



Cloudflare 1.1.1.1 incident on June 27, 2024

2024-07-04

Introduction

On June 27, 2024, a small number of users globally may have noticed that 1.1.1.1 was unreachable or degraded. The root cause was a mix of BGP (Border Gateway Protocol) hijacking and a route leak.

- Trade-off between operability vs attack surface reduction.
  - Attacks can bypass RPKI.
- RPKI interferes with other routing practices (e.g. DDoS blackholing)

RPKI can be a vector of attack

The Hacker News

Subscribe – Get Latest News

Home Cyber Attacks Vulnerabilities Expert Insights Contact

Orange Spain Faces BGP Traffic Hijack After RIPE Account Hacked by Malware

Jan 05, 2024 Ravie Lakshmanan

Massimo Candela Follow

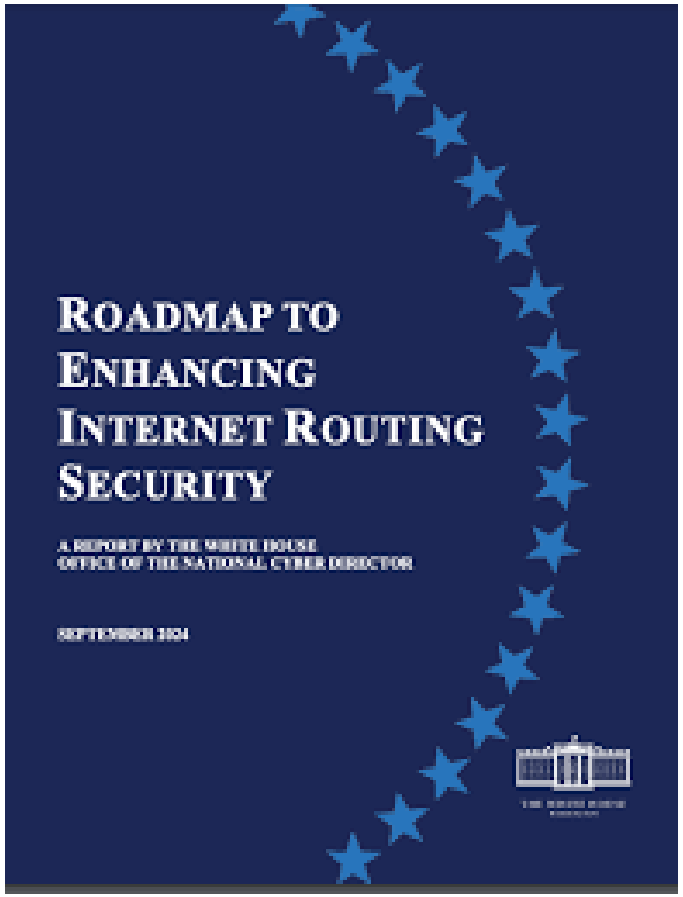
RPKI Trust Anchor Malfunctions: A Review of the Last 3.5 Years

RSAC™ 2025 Conference

Law and Policy

Two Major Recent Federal Initiatives

ONCD Roadmap



FCC NPRM

51284 Federal Register / Vol. 89, No. 117 / Monday, June 17, 2024 / Propos

Dated: June 11, 2024.
Lauren K. Roth,
Associate Commissioner for Policy.
[FR Doc. 2024–13236 Filed 6–14–24; 8:45 am]
BILLING CODE 4164–01–P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 1

[PS Docket Nos. 24–146, 22–90; RIN 3060–AL83; FCC 24–62; FR ID 225236]

Reporting on Border Gateway Protocol Risk Mitigation Progress; Secure Internet Routing

AGENCY: Federal Communications Commission

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) seeks to increase the security of the information routed across the internet by proposing certain reporting obligations on providers of broadband internet access service (BIAS providers) and their use of the Border Gateway Protocol (BGP). Internet traffic can be disrupted, intercepted, and blackholed—when a service provider drops traffic addressed to a targeted IP address or range of addresses by redirecting it to a null route—due to either accidental or deliberate adversarial manipulation of security vulnerabilities inherent to BGP. Together, the intended effect of the plans, filings, and measures the Commission proposes would be to mitigate such threats. BIAS providers would be required to develop BGP Routing Security Risk Management Plans that describe their plans for and progress in implementing security measures that utilize the Resource Public Key Infrastructure (RPKI). Nine of the largest service providers would be required to file specific additional data on a quarterly basis. The FCC also seeks comment on issues related to implementing RPKI-based security measures.

DATES: Comments are due on or before July 17, 2024 and reply comments are due on or before August 1, 2024.

- *Federal Communications Commission's website: https://www.apps.fcc.gov/ecfs/.* Follow the instructions for submitting comments.
- *Mail:* Parties who choose to file by paper must file an original and one copy of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number. Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission. Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701. U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street NE, Washington, DC 20554.

Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID–19. *See FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy,* Public Notice, DA 20–304 (March 19, 2020). *https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy.*

People with Disabilities. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an email to *fcc504@fcc.gov* or call the Consumer & Governmental Affairs Bureau at 202–418–0530 (voice), 202–418–0432 (TTY).

FOR FURTHER INFORMATION CONTACT: George Donato, Associate Division Chief, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418–0729, or by email to *george.donato@fcc.gov;* or James Zigouris, Attorney-Advisor, Cybersecurity and Communications Reliability Division, Public Safety and

ONCD Roadmap: Origins

ONCD Roadmap: Key Elements

- Raising priority of the issue, pushing for wider RPKI adoption
- Creation of public-private working group
- Recommendations: federal government
- Recommendations: baseline ones for all network operators
- Recommendations: additional ones for network service providers

ONCD Roadmap: Current Efforts

- Executive Order 14144 (Jan. 16, 2025)
- Secure Internet Routing Working Group
- NIST Special Publication 800-189r1 ipd

FCC NPRM: Background

FEDERAL COMMUNICATIONS COMMISSION

[PS Docket No. 22–90, FCC 22–18; FRS 75229]

Secure Internet Routing

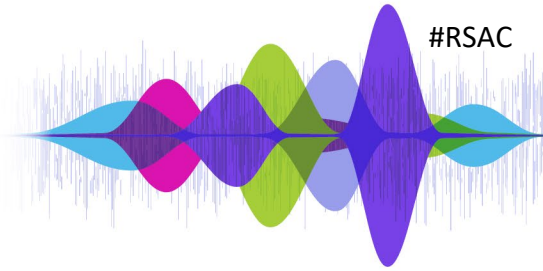
AGENCY: Federal Communications Commission.

ACTION: Request for comments.

SUMMARY: In this document, the Federal Communications Commission (FCC or the Commission) seeks comment on vulnerabilities threatening the security and integrity of the Border Gateway Protocol (BGP), which is central to the Internet's global routing system, its impact on the transmission of data from email, e-commerce, and bank transactions to interconnected Voice-over Internet Protocol (VoIP) and 9–1–1 calls, and how best to address them.

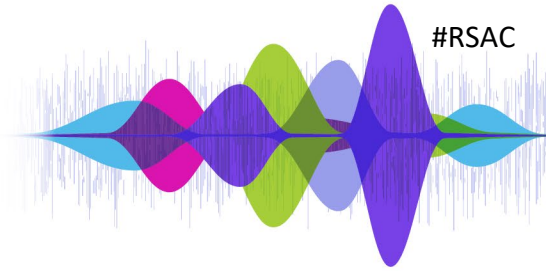
DATES: Comments are due on or before April 11, 2022; and reply comments are due on or before May 10, 2022.

FCC NPRM: Key Elements



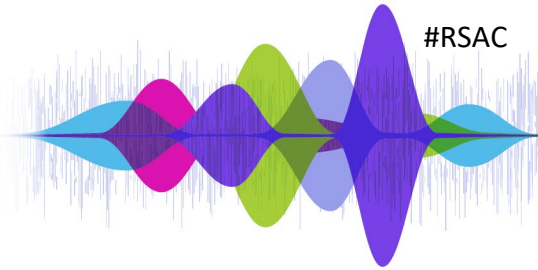
- **Require certain large service providers to file initial BGP Plans:**
  - detailed description of the service provider's process for assessing and prioritizing the creation and maintenance of ROAs
  - If service provider does not control the IP address prefix(es) in question:
    - describe status of ROA registrations for routes they originate;
    - explain the reason(s) why the service provider is unable to register particular sets of IP prefixes;
    - describe in detail the service provider's efforts and plans for facilitating ROA registrations for the IP prefixes that have been transferred and not under its control

FCC NPRM: Key Elements



- **Require certain large service providers to file initial BGP Plans (cont'd):**
  - describe the extent to which it has implemented ROV filtering at its interconnection points with its peers as well as its customers, and to what extent ROV has been disabled or not deployed within its network

FCC NPRM: Key Elements



- **Subsequent BGP Plans:**
  - Unnecessary if attestation service provider has registered and maintained ROAs covering at least 90% of originated routes for IP address prefixes under its control
- **Quarterly BGP security information filings**
- **Service Providers Other than the Largest Providers:**
  - Make BGP Plans available upon staff request

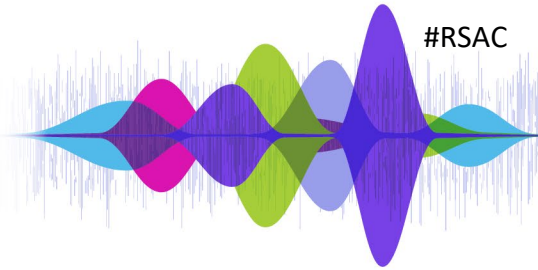
FCC NPRM: Responses

- 20 comments, representing 30 companies, organizations, or individuals
- 10 reply comments
- Some common themes:
  - Avoid prescriptive regulation
  - Work through international multistakeholder organizations
  - Need to look beyond RPKI
  - Clarify coverage and scope of proposed reporting obligations

FCC NPRM: Uncertain Future

- **Legal Basis**
- **Trump Administration Position?**

Looking Outside the United States



- **OECD?**
- **Multi-stakeholder Forums?**

“Apply” Slide

- What are the routing security practices of your Internet connectivity provider?
  - Is your address space covered by RPKI Route Origin Authorizations?
  - Has your provider implemented RPKI Route Origin Validation?
- Internet Service Providers:
  - Check the status of your RPKI implementation (ROA & ROV)
  - Do you support customer issuance of RPKI certificates?
  - Do you monitor the BGP routes you receive and accept?
- Engage with peers through an initiative (e.g. MANRS, CableLabs, Internet2, …)

RSAC 2025 Conference

Many Voices.
One Community.

Cecilia Testart

ctestart@gatech.edu

Jonathan Cedarbaum

jonathan.cedarbaum@law.gwu.edu